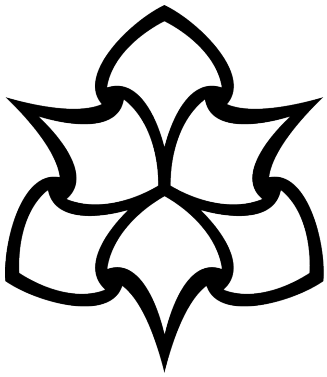

IoT, Internet of Things, Security, Cyber Security, Secure by Design, Next Generation Internet, Smart City, Sustainable City, Energy Reduction, Building Energy Management Systems

Internet of Things: Evolution and Technologies from a Security Perspective

Abstract

In recent years, IoT has developed into many areas of life including smart homes, smart cities, agriculture, offices, and workplaces. Everyday physical items such as lights, locks and industrial machineries can now be part of the IoT ecosystem. IoT has redefined the management of critical and non-critical systems with the aim of making our lives more safe, efficient and comfortable. As a result, IoT technology is having a huge positive impact on our lives. However, in addition to these positives, IoT systems have also attracted negative attention from malicious users who aim to infiltrate weaknesses within IoT systems for their own gain, referred to as cyber security attacks. By creating an introduction to IoT, this paper seeks to highlight IoT cyber security vulnerabilities and mitigation techniques to the reader.

The paper is suitable for developers, practitioners, and academics, particularly from fields such as computer networking, information or communication technology or electronics. The paper begins by introducing IoT as the culmination of two hundred years of evolution within communication technologies. Around 2014, IoT reached consumers, early products were mostly small closed IoT networks, followed by large networks such as smart cities, and continuing to evolve into Next Generation Internet; internet systems which incorporate human values. Following this evolutionary introduction, IoT architectures are compared and some of the technologies that are part of each architectural layer are introduced. Security threats within each architectural layer and some mitigation strategies are discussed, finally, the paper concludes with some future developments.

1. Introduction

The Internet of Things (IoT) is a network of everyday things, connected together through the Internet. The function of an IoT system is to monitor the world around itself, to enable and assist, or to automate a response to changes in the system's environment [118, 25]. In comparison, the purpose of an IoT system is to improve the quality of life by enabling the best response to an environmental change [79] by

providing responsive services which are specific to the end-users' needs [88]. An IoT device can be 'any thing' in the world that includes the technological components to enable the Thing to connect to the Internet through a wired or wireless network. IoT users can be a human, or machine, or a combination [20]. IoT is not a specific device or technology, instead, IoT is the inter-working of different technologies enabling the connectivity of many Things.

Generally, IoT networks comprise of many connected Things connected together through a management platform. The platform has a number of roles including managing the connected Things, system threats and security, data analysis, processing and storage, and managing the response of any Things [46]. IoT Things can either have all of their electronic components included in them at conception, or added later. Examples of systems where smart functionality is added after conception [81] include a pet with a tracking tag, external or implanted human biometric systems, or older high value legacy vehicles such as an aircraft. Smart conceptualised systems include smart home heating and self-driving vehicles.

2. Evolution of ICT Culminating in IoT

Figure 1 is a time-line showing the evolution of Information Communication Technologies (ICT) starting from the 1830s, highlighting some of developments and culminating in IoT. The telegraph is considered as the first major invention of wireless communication technology. Following this hugely significant invention, comes the creation of the telephone, closely followed by the birth of computers. The invention of computers in the 1920s enabled the solving of complex computations, including the breaking of previously unbreakable codes and calculations including code breaking at Bletchley Park during WWII. The architecture of this early machine became the foundation for the computing theory that followed [92]. This led on to the development of the Personal Computer (PC) in the 1970s, and their unprecedented uptake in the 1980s. The PC totally revolutionised the lives of individuals in the home and workplace due its reduction in size and cost, and the addition of new software such as word processing and spreadsheet tools [75]. Computer technology has developed relatively slowly over 90 years to the computers we recognise today, from large powerful servers, to PCs and more versatile mobile computers, including the laptop, tablet and smart phone.

The next development along the time-line was the networking of computers, including US Defence Department project ARPNET, through to the WWW, developed by Tim Bernes-Lee and launched in 1991 as a tool to share documents. The combination of the Internet and WWW are the most significant milestone within the IoT

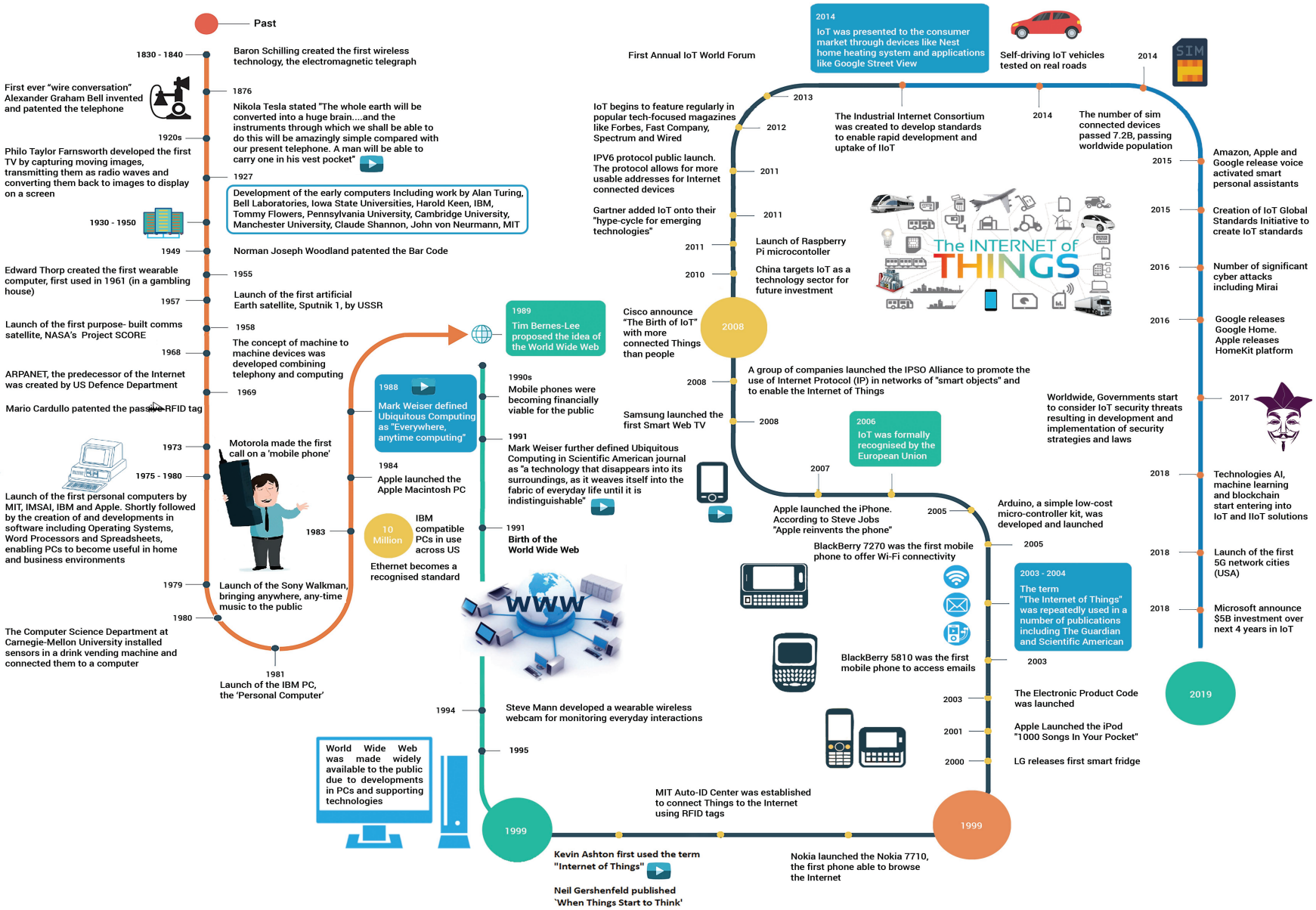

Figure 1: Time-line: The Evolution of ICT Culminating in IoT

time-line. Similar to computers, the Internet has developed relatively slowly, over 50 years from closed connectivity projects to the powerful tools that we all know and use today.

The release of the Raspberry Pi microcontroller in 2011 was another major IoT breakthrough and was in-part responsible for the swift uptake of IoT technology. This low-cost, versatile microcontroller suddenly opened up IoT to hobbyists and end users. Other microcontrollers did exist, but due its low cost, low complexity and relatively large processing power and significant amount of free on-line support, including tutorials, videos, educational DIY websites, blogs and forums, IoT was no longer limited to commercial projects. The time-line continued onto 2014 when IoT technology was widely presented to the consumer market by companies like Google, as they acquired Nest, Apple introducing the Apple Watch, and Siemens as they introduced SmartThings, an affordable smart home starter kit and software platform.

Since this consumer introduction, IoT has continued to develop significantly, including the creation of more than 400 IoT platforms, many commercial IoT developers and thousands of products. In 2016, large tech companies including Amazon, Apple and Google have release voice activated personal assistants. In addition to consumer IoT, there is Industrial IoT (IIoT) enabling the automation of many industrial processes. The concept of IoT has also continued to evolve; initially IoT systems comprised of lots of small closed networks, but this concept has evolved to incorporate larger more connected networks, for example smart cities with smart transport infrastructures. But large infrastructure is not the end of this evolutionary journey, the concept of IoT is currently evolving into the Next Generation Internet (NGI). NGI is the vision of IoT which seeks to encompass human values within Internet based systems, enabling "human potential, mobility and creativity at the largest possible scale while dealing responsibly with our natural resources... we shape a value-centric, human and inclusive Internet for all" [60]. These NGI concepts are being integrated into existing and new IoT systems through the inclusion of advanced technologies such as artificial intelligence, machine learning, augmented reality and virtual reality, are others, whilst "making the future internet more human-centric". In many areas, NGI concepts match the smart sustainable city concept, the main difference is NGI includes human values of well being, rather than just environmental and economical well-being.

Alongside of this evolutionary journey, in 2016 and 17, there were a number of very significant security attacks, particularly the Mirai Dyn attack and WannaCry NHS attack. In response, world wide Governments have begun developing strategies, initiatives, and in some instances, laws to strive to reduce IoT security vulnerabili-

ties. Other technologies including Artificial Intelligence (AI), machine learning and Blockchain are being combined with IoT to produce more powerful tools. Similarly, Augmented Reality (AR) and Virtual Reality (VR) technology are being combined to with IoT to create a more interactive user experience.

This evolution of ICT technology, which culminated in IoT has taken 200 years. In comparison, from the initial concepts of IoT in 1999, through to introduction of IoT to the consumer around 2014, which has led onto widespread adoption of IoT technology. The IoT development cycle is just 15-20 years and as a result of this rapid development, IoT faces major issues, the most significant of which are security vulnerabilities. The severity of IoT security vulnerabilities are because security has been a developmental afterthought. Designers, developers and policy makers worldwide are now looking for ways to reduce this issue. In 2018 the British Government released the world's first IoT code of practice entitled 'Secure by Design' [36]. This code aims to "remove the burden from consumers to securely configure their devices and instead ensure that strong security is built into IoT devices and services by design" [35], also the British Government is currently consulting over whether to mandate security laws for IoT consumer products [37]. Other related methodologies, strategies and technologies are also being researched and developed [121, 104, 23, 80]. Additionally, the British Government is investing 30.6 million into 'Security of Digital Technology as part of the the Periphery' (SDTaP) research program. This investment has included the opening in March 2019 of The PETRAS (privacy, ethics, trust, reliability, acceptability, and security) National Centre of Excellence for IoT Systems Cybersecurity. The national centre of excellence is a collaboration between a number of universities, including Imperial College London, Bristol University and 150 industrial partners.

3. Related Work

There is a large number of tutorials, surveys and research studies in the area of IoT. Significant surveys [16, 5, 77] consider IoT concepts and technologies as a whole, including the architectures, technologies and principal applications of IoT. Atzori et al. [17], develops his earlier survey [16], challenging the popular idea that IoT can be used to solve any issue. Many real IoT smart city deployments are detailed and analysed, including these works [2, 126, 83].

Further works focus on technologies or challenges within IoT systems, these include works comparing IoT architectures [127, 85, 5, 125]. Specific communication technologies [5] are defined and compared. Hejazi et al. [54] compare IoT cloud platforms defining strengths, weakness and where they each fit within the IoT sector.

Similarly, IoT Operating Systems (OS) are detailed and compared [24, 30]. Bujari [26] considers current challenges including interoperability, security, privacy, and business models. Security challenges are studied [124, 44, 7] and Alaba [7] surveys existing security solutions. Stergiou [115] surveys IoT and Cloud Computing from the perspective of security, Yang et al. [124] and Granjal et al. [47] both study IoT security vulnerabilities and analyse the effectiveness of security strategies. Gupta et al. [50, 51] have created a number of security books including a practical and detailed handbook which surveys security across a range of ICT including wired and wireless systems, ad-hoc networks, human wearables and cloud computing. The second [51] is a comprehensive book covering security trends, cyber risk, vulnerability assessments, the human factor, smart phone protection, critical infrastructure protection. It also introduces security policies and techniques including cryptography, standards and modelling.

The contributions of this paper relative to existing literature can be summarised as this paper is written with:

- Consideration of practitioners and researchers from neighbouring fields.
- A brief history and overview of the evolution of IoT, demonstrating where IoT sits within ICT and current trends including Industrial IoT, Smart Cities and Next Generation Internet.
- Consideration of IoT security vulnerabilities.
- Recommendations to reduce security threats.
- Architecture and technologies are considered from the perspective of designing, developing and securing large Next Generation Internet IoT systems, this includes quick reference technology comparison tables (Tables Table 1, Table 2, and Table 3).

4. IoT Technologies

IoT is not a single technology, but a system or framework comprised of many technologies. This section will begin by considering some definitions of IoT and then introduce three IoT architectures, before looking in more detail at one specific architecture, considering the the technologies and security vulnerabilities within each of its layer. Some security attacks that can be applied to IoT systems including node capture, eavesdropping, malicious control, IP Spoofing, Ping of death, sniffing, malicious code injection and denial of service. These attacks will be discussed and

mitigation techniques suggested. Technologies within IoT systems including Things, communication technologies, management platforms, data management tools and user applications will also be introduced.

4.1. Definitions and Concepts

The IEEE has developed two definitions of IoT [87, 56], the first is with respect to simple IoT networks, and states:

"An IoT is a network that connects uniquely identifiable "things" to the Internet. The "things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "thing" can be collected and the state of the 'thing' can be changed from anywhere, anytime, by anything."

The second definition is specific to larger networks, for example smart cities, and it states:

"Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."

From both of the definitions, a number of characteristics can be highlighted:

1. IoT is a system that incorporates and connects 'Things'
2. Things sense or monitor their environment
3. Things connect to the Internet to communicate
4. Things are uniquely identifiable
5. The system can potentially compute data, for example use, process, store or transmit data onward
6. The system should present information to a user or multiple users
7. The system responds to input from connected Things and, or users

.

The National Institute of Standards and Technology (NIST) do not define IoT, instead they state some of the characteristics of IoT. These characteristics resemble the IEEE definitions. NIST state that IoT systems "involve sensing, computing,

communication, and actuation" [120]. Inline with these definitions [56], and others [120, 12, 43, 59, 16, 42, 91, 40, 33], Internet connected enterprise infrastructures, PCs, laptops, tablets and smart phones will be considered part of IoT.

IoT has use-cases in many areas of life, but in the last few years the focus of IoT has been moving away from small, independent and unconnected networks towards more joined-up infrastructures and networks, particularly with a focus on smart cities. In 2016, the ITU-T SG20 IoT working group changed its name to 'ITU-T SG20: Internet of things (IoT) and smart cities and communities (SCC)'. This group is currently developing 83 smart city standards, each focused on a different aspect of smart city infrastructure such as architecture [65, 66, 69], data sharing [64] or security [67, 68]. Similarly, the IEEE P2413 IoT working group has created a smart city group, IEEE P2413.1. They are currently developing 'P4213.1 Standard for a Reference Architecture for Smart City (RASC)' [13].

The concept of smart cities and sustainable cities have been around since the mid 1990s [70]. Initially, smart cities simply referred to cities with economic improvement strategies, next the concept included use of ICT within city infrastructures, later the concept became more citizen centric. Today, most stakeholders would agree that smart cities include technology in their infrastructures, enabling them to serve their citizens, providing "more efficient services to citizens, to monitor and optimize existing infrastructure, to increase collaboration amongst different economic actors and to encourage innovative business models in both private and public sector" [82]. In addition to the well being of citizens and city infrastructure, the environmental sustainability of a city's operations has also become an important feature, "Cities become smart sustainable when smart ICT is employed for making them (the cities) more sustainable" [22]. A more recent concept is that of Next Generation Internet, in combination with smart sustainable cities, resulting in 'Next Generation Sustainable Cities'. There are a number of important characteristics of these cities. Firstly, next generation sustainable cities seek to "shape the future internet as an interoperable platform ecosystem that embodies the values .... openness, inclusivity, transparency, privacy, cooperation, and protection of data" [60]. Secondly, next generation sustainable cities are 'next generational', the technology they are comprised of is developed based upon the analysis of previous and existing generations of the technology [95]. Thirdly, next generation sustainable cities are built with next generation technologies, for example, 5G telecommunications, intelligent technologies including machine learning and AI. Thirdly, NG sustainable cities are are citizen centric, promoting the health and well-being of all citizen, the city and its environment impact and sustainability.

4.2. Architectures

A technical architecture is a framework created to allow designers and developers to consider the system as a whole and also to break it down into sections. According to Global Standards 1 (GS1),"a reference architecture is an essential foundation to enable integrating the diverse technologies into IoT applications" [48]. There are many groups working on developing IoT architectures and other standards. These groups include IEEE P4213 Working Group, IEEE 802.24 Technical Advisory Group (TAG), IEEE P4213.1 Working Group, The National Institute of Standards and Technology (NIST) IoT Working Group, International Standard Organisation / International Electrotechnical Commission (ISO/IEC) 30141 JTC1 IoT Working Group 10, International Electrotechnical Commission Strategic (IEC) Group8, International Telecommunication Union Telecommunication (ITU-T) Group, oneM2M Consortium, Open Connectivity Foundation (OFC), Industrial Internet Consortium (IIC), and Internet Engineering Task Force (IETF). Though currently, none of these architectures are universally accepted, so below three architectures will be considered and compared.

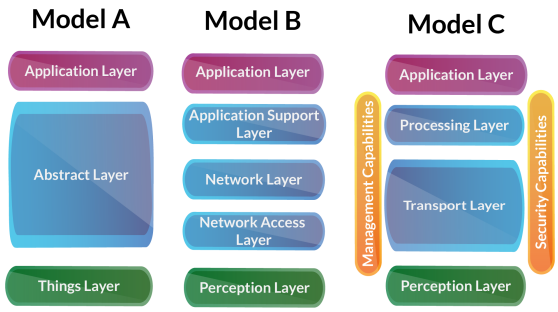

Figure 2: IoT architectures: (A) IEEE P4213 Three Layer Architecture [14]. (B) Zhong [127], Miao Wu [85] and Montagero's [90] Five Layer Architecture. (C) ITU-T Y.4000 Four Layer Architecture [41].

Historically, the most common IoT architecture is the Three Layer Architecture, illustrated in Figure 2-A. This framework is currently being developed further as part of the IEEE P4213 IoT architecture standard [14] which is based on the SO/IEC/IEEE 42010-2011 systems and software engineering architecture description standard [63]. The same framework is expanded upon within the IIC's industrial internet of things reference architecture [78]. Similar architectures are discussed [16, 85, 5]. This architecture comprises of the Things, Abstract and Application Layers [14, 107, 10]. The IEEE P4213 standard is open source and is a widely

accepted and supported standard which has been in development for a number of years, and is still being developed. The standard is very detailed, comprising over 100 pages with the aim of creating an architectural framework which is relevant to any industry or use case. Though, some researchers [127, 6] suggest the Three Layer Architecture is too high level and does not allow the different components of the IoT system to be separated out sufficiently to enable system development or protection. For the purpose of this paper, considering IoT from a security perspective, the authors agree with this conclusion, that further division of the IoT system will enable easier consideration of the security vulnerabilities. The next architecture considered is the ITU-T Y.4000 Overview of the IoT [41]. This standard comprises of a 4 layer architecture, with separate over-arching management and security capabilities, as shown in Figure 2-C. Again, for the purpose of this paper, it is more helpful to consider security within each architectural layers, rather than separating security out. In 2015 a group of researchers, Zhong et al. [127], introduced a Five Layer Architecture comprising of the Perception, Network Access, Network, Application Support and Application Presentation Layers, illustrated in Figure 2-B. Similarly in 2017, Montagero et al. [90] and Miao Wu et al. [85] developed an architecture based on the computer networking Open System Interconnect (OSI) technology architecture. Montagero et al.'s architecture resembled that developed by Zhong et al. Miao et al.'s architecture comprised of the same five layers as Zhong et al.'s, plus an additional Business Layer. From this point forwards, this architecture will be referred to as Zhong's Five Layer Architecture

Summary of the Architecture Layers:

1. The lowest layer, commonly referred to as the Perception Layer is the same across all three architectures and comprises of the physical layer that interfaces between the physical and information world, monitoring the environment and collecting data. The layer comprises of hardware devices including sensors and actuators. In this layer, the collected data is converted into digital data, ready for transmission up, to the next layer.
2. As can be seen from Figure 2, the Abstract Layer in Model A is subdivided in Model B and C. The Network Access Layer (Model B) is concerned with moving the digital data from the perception layer to an access node or gateway. The data is transmitted using access technologies like Ethernet, Wi-Fi, Bluetooth or Zigbee. The data is then ready to be used in the Network Layer.
3. The Network Layer (Model B) is concerned with transmitting data received at the access node throughout the whole IoT network, including the Application Support Layer and the Application Presentation Layer. These transmission technologies can include wired and wireless Internet protocols, for example

HTTP, MQTT and CoAp. In ITU-T's architecture (Model C), the Transport Layer is a combination of the Network Access Layer and Network Layer of Zhong's architecture (Model B).

4. The Application Support Layer (Model B), also referred to as the Processing Layer (Model C), is responsible for processing data. Dependant upon the size of the IoT system, this layer can be very complicated as it is responsible for processing and combining data from many different sensors and other devices and presenting it ready for use in the Application Layer. Technologies within this layer can include management platforms and technologies responsible for data processing, analysis and storage, this can include cloud technologies.
5. The Application Layer allows the end-user to make use of the collected data. The layer comprises of tools to develop and manage end-user applications. These applications are commonly referred to as 'Apps' which deliver IoT end-user services, for example health monitoring tools, smart homes or smart city applications.
6. Miao Wu et al.'s Architecture differs slightly from Zhong's Architecture because it includes an additional layer, the Business Layer. This layer can be considered as the "manager of the Internet of Things" [85], concerned with business and profit models, management of data sharing [5], software updates and system interoperation. This layer is very important and must be considered in the design and development of an IoT system, particularly within large systems such as smart cities. Miao Wu et al. explain that the success of a technology does not only depend on development of the technology, but also the innovation and development of the business models that manage how the technology will be used. Based on this point, the Internet of Things may not have long-term future without the significant development of its business models [85]. This layer is outside of the scope of this paper.

.

Throughout the rest of the paper, when an architecture is referred to, it is Zhong's Architecture, labelled Model B in Figure 2. When considering the movement of data throughout all of the layers of the architecture, it is important to highlight that data can move in the opposite direction to that explained above, from the Application Layer back down to the Perception Layer, enabling actuators to respond to collected data, system instructions or end-user instructions.

Other well referenced architectures include the oneM2M IoT architecture [117], cloud centric architecture [49], software stack architecture [113], TCP/IP architecture, OSI reference architecture [85] and Representational State Transfer Services

(RESTFUL) architectural style linked to HTTP [72]. Next, the paper will look in more detail at the technologies that exist within each of layer of Zhong's architecture.

4.3. IoT Technologies within the Perception Layer

As defined earlier, the end point of an IoT system is the 'Thing' that interacts with itself, other Things or its environment [14]. Generally, the Thing is collecting, responding data from the physical world or responding to instructions from the IoT system. The technology in is this layer is shown in Figure 3 and comprises of the hardware and software components that enable any physical object to act as an IoT Thing.

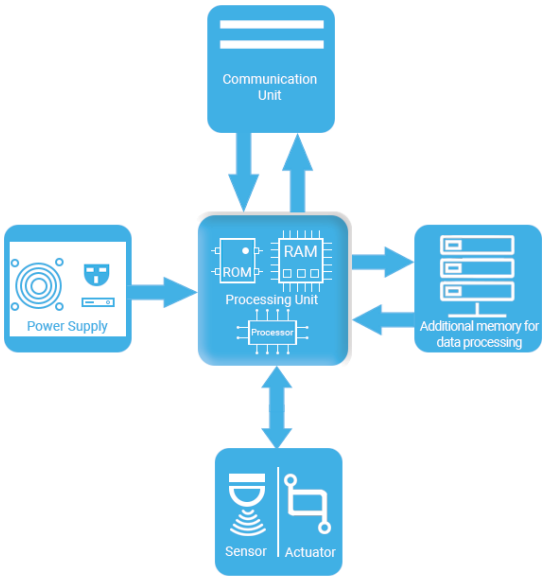

Figure 3: Components of an IoT Thing

4.3.1. Sensor & Actuator Unit

Sensors and Actuators are electrical components that connect the real and digital world by monitoring or responding respectively. Sensors are input components that monitor environmental characteristics and convert changes in this characteristic into an electrical signal. The relationship between environmental characteristics and electrical signal outputs can be linear or non-linear, this relationship is defined within the sensor's specifications.

Actuators are output components. They create a physical response to a change in their electrical input. Generally actuators fall into four categories based on the nature of their physical response:

- Hydraulic - moving under pressure liquids through a defined space
- Pneumatic - using gas stored under pressure
- Electric - generating electricity
- Mechanical - operating machinery

Similar to sensors, the relationship between electrical signal and actuator output is defined within its specifications. Generally, IoT sensors and actuators are small in size, low complexity and low unit cost. In some system, particularly critical infrastructure systems, higher specification sensors or actuators may be required, this can increase the cost of these components. Examples of component specifications include fault tolerance, sensing resolution, sensing rate, response rate, sensing range, magnitude of response, accuracy, security, storage or processing capabilities. When designing a system, component specifications and cost are important considerations.

4.3.2. Processing Unit

The processing unit is comprised of hardware and software that manage the behaviour of the Thing. This unit is commonly a microcontroller; a small, simple, programmable, self-contained computer on a single integrated circuit comprising of a processor, ROM, RAM and IO. Some microcontrollers that are commonly used with IoT projects and have significant amounts of development support.

A microcontroller is usually built and programmed to carry out simple tasks related to a single simple function, for example, controlling a smart fridge. They can be built into more complex devices, for example smart phones, then they are referred to as 'embedded'. Due to their constrained specifications, microcontrollers can not run traditional operating systems, instead they use constrained operating systems, for example mBed, TinyOS or rasbarian [102]. A microcontroller can have additional memory added to enable it to execute additional processing tasks, for example, to carry out data processing or data analysis at the sensor to reduce the amount of data transmitted from the sensor to the IoT network. This is sometimes referred to as 'edge' analysis. Additionally, the microcontroller can include security features such as data encryption and endpoint authentication.

4.3.3. Communication Unit

This unit is responsible for transferring or receiving data. If data is collected at the sensor, the communication unit will transfer the data to the IoT network. Alternatively, if data is received from the IoT network, it will then be acted upon by the actuator. Communication technologies are considered in more detail in Section 4.4. Generally microcontrollers have communication unit inbuilt, so when choosing a microcontroller, the communication and security requirements of the IoT system must be considered, for example, the desired data transfer rate and transfer distance. These requirements will also affect which communication technology is most suitable, for example for a contactless card payment system, the most suitable technology is Near-Field Communication (NFC) RF technology with a transfer distance of $10cm$. Within the IoT endpoint, communication consumes the largest proportion of power, therefore the communication technology also affects the power supply requirements.

4.3.4. Power Supply

Endpoint power requirements vary significantly dependant upon the energy requirements of all of the above components. If the Thing is connected to a mains power supply, the power requirements of the Thing can be considered nearly negligible in comparison. If the Thing is fixed in one location, for example a smart fridge, the power supply would generally be wired, for example to the mains power supply. Often though, IoT endpoints are mobile, meaning a wired power supply may not be suitable. Instead for mobile endpoints, power could be supplied from a portable source, for example batteries or a renewable source, for example solar panels or an energy harvesting unit. According to Andersen, for a wireless IoT system to be commercially viable, each Thing should have a power supply lifetime of $5 - 10$ years [11].

The criticality of an IoT system must be considered when selecting a power supply. For a highly critical system, for example a warning system within a power plant, the reliability, redundancy and security of the power supply and its connection must be considered. In this example, solar power is unlikely to be selected as the only power supply. Instead, multiple power supplies may be connected via multiple techniques to provide sufficient confidence.

4.4. IoT Technologies within the Network Access Layer and Network Layer

The movement of data within a network is referred to as communication, similarly, terms 'connect', 'transfer' or 'transmit' can be used. Within Zhong et al's architecture, the communication of data is be broken into two categories; access communication technology which sits within the Network Access Layer, and network

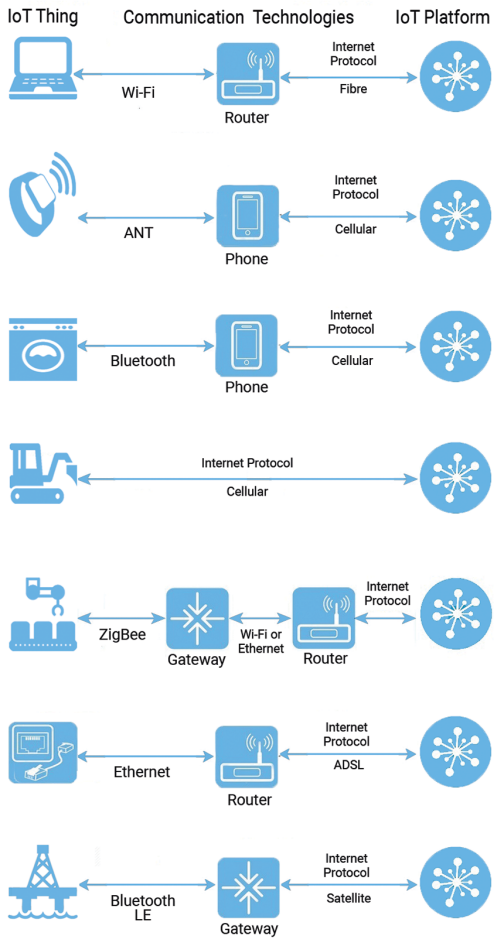

Figure 4: IoT Short to Medium Range Communication Configurations

communication technology which sits within the Network Layer. Access communication technologies connect the IoT Thing to the IoT network, usually achieved by transmitting data from the IoT endpoint to a network access gateway. The network communication technologies transmit data around the rest of the IoT network, from the access gateway all the way to the Application Layer. These communication technologies are the where most IoT security vulnerabilities exist. Figure 4 is an illustration of some short to medium range communication configurations, demonstrating technologies from the Perception, Network Access Layer and Network Layer. This illustration is not an exhaustive list of technologies or configurations.

4.4.1. Access Communication Technologies

Sometimes IoT networks are oversimplified to only include wireless networks, but this is wrong, IoT networks can be wired too. Wireless networks are commonly used in hard to reach or hard to install environments, or where wired network installation is more costly. Conversely, wired networks may be used where the wired infrastructure already exists, higher data throughput or increased security is required.

Due to power supply restrictions, wireless networks should be designed to have low power requirements. This means wireless networks are well suited to systems with short transmission distances and low transfer rates. The choice of which communication technology and protocol to choose is generally based on the system requirements, including:

- Wired / wireless
- Data rate
- Data reliability
- Data security
- Proximity of the Thing to receiving node
- Nature of environment
- Ease of access / maintenance
- Number of connected Things
- Number of simultaneously active Things
- Overall system size and complexity

	TECHNOLOGIES						
	Bluetooth	Bluetooth Low Energy	ANT	Wi-Fi	NFC	Zigbee	Z-Wave
Range (m)	100 m	50-100 m	30 m	30-50 m	5-10 cm	10-100 m	30 m

Table 1: Wireless Short to Medium Range Communication Technologies (Continued over page)

Bwidth (Hz)	2.4 GHz	2.4 GHz	2.4 GHz	2.4 / 5 GHz	13.6 MHz	2.4 GHz	2.4 GHz
Data Rate (bps)	1-3 Mbps	125 Kbps - 1 Mbps	12-60 Kbps	150-200 Mbps	100-420 Kbps	250 Kbps	9.6, 40 or 100 Kbps
Battery Lifetime	0.6 Ah: Standby: 3 mnth. Mixed: 5 dy	1 Ah: Mixed: 1-2 yr. 2xAA: 14 yr	1 Ah: Mixed: 15 yr	2xAA: Listening: 2 dy	Initiator trf: 15 mAh. Passive: 0 mAh	2xAA: Mixed: 5 yr	2xAA: Mixed: 1 yr
Authentic^{n}	Yes	Problematic	Yes	Yes	Yes	No	Yes
Encrypt^{n}	Yes	Yes	No	Yes	Yes	Yes	Yes
Standard	Based on IEEE 802.15.1	Bluetooth 4.2	Proprietary	IEEE 802.11	ISO/IEC 14443, 18092	IEEE 802.15.4	Z-Wave Alliance Proprietary
Scalability	Yes	Yes	Yes	No	No	Yes	Yes
Topology	P2P, Star (Piconets)	P2P, Star (Piconets)	P2P, Star, Tree, Mesh	P2P, Star	P2P	Mesh	Mesh
N^{o} Nodes (Mst : Slv)	8 (1:7), (200 inactive slv)	8 (1:7) (32K inactive slv)	65533 (per 8 channels)	255	2	232	232

Table 1: Wireless Short to Medium Range Communication Technologies [21] [1] [114] [123]

Defining a communication technology typically defines two elements; firstly, the nature of the transmitted data signal, and secondly the material through which the signal is transmitted. For example, Ethernet technology comprises of an electrical

signal transmitted along an Ethernet cable. For Bluetooth technology, an electromagnetic RF signal is transmitted through air at 2.4GHz. Communication technologies that do not require a wired medium are referred to as wireless.

Communication protocol refers to the rules that define how the data should be transmitted, for example, the number of bits in a data packet, which bits are real data and which are management data. Management data is generally transmitted as a data header or footer, and used to control the flow of data, including, defining the destination address, and how the data should travel to the destination.

	TECHNOLOGIES					
	Cellular 3G	Cellular 4G	SigFox	LoRa	NB-IoT	LTE-M
SPECS						
Urban Range (Km)	5 - 8 km	15 km	3 - 10 km	2 - 5 km	9 km	11 km
Rural Range (Km)	50 - 70 km	45 km	30 - 50 km	15 km	unavailable	unavailable
Transm^{n} Bandwidth (Hz)	800 MHz - 2.4 GHz	800 MHz - 2.6 GHz	868 MHz	850 MHz - 1 GHz	200 KHz, 700 - 900 MHz	700 - 900 KHz, 1.4 MHz
Data Rate (Kbits/s)	Mobile: 128, 144 Kbps. Fixed: 2 Mbs	Mobile: 20 - 100 Mbps	0.3 Kbs	0.3 - 50 Kbs	150 Kbs	64 - 128 Kbs
Power (mAh)	460 mAh	600 mAh	32 - 51 mAh	40 mAh	unavailable	80 mAh

Table 2: Wireless Wide Area Communication Technologies (Continued over page)

Standards	UMTS, HSPA, W-CDMA, WLAN, WiMAX,	OFDM, CMDA, WiMAX, LTE, LTE Adv	Proprietary	Proprietary	SC-FDMA, PRACH	OFDM, PRACH
Uses	Messaging, Internet, VoIP, IPTV	Messaging, Internet, VoIP, Games, Cloud	IoT systems	IoT systems	IoT systems	IoT systems
Battery Life	hours - days	hours - days	5 - 10 years	10 years	>10 years	>10 years

Table 2: Wireless Wide Area Communication Technologies [15] [76] [97] [94] [122] [119] [31]

For an IoT network spanning a few meters, across a single building, or collection of buildings, short to medium-range communication technologies should be selected. Communication technologies can be categorised based on their network range and use. These categories include the body area network (BAN), personal area network (PAN), local area network (LAN) and wide area network (WAN) technologies. BAN technologies include Ant, PAN technologies include NFC, Bluetooth, Bluetooth Low Energy, Zigbee and Z-wave. LAN technologies include Wi-Fi and Wi-Fi Low Energy, additionally Ethernet is a wired LAN technology. Some wireless short to Medium range technologies are compared in Table 1.

Many IoT systems, particularly larger networks, utilise numerous access communication technologies to connect multiple Things to the network. For an IoT system that covers a larger area, for example a Smart City, short and medium-range communication technologies may not be suitable to connect all of the endpoints to the network [29, 110]. Wired and wireless WAN technologies can be used. Significant work by Centenaro et al. considers cellular and low power WAN technologies, creating networks that span $10 - 50km$ in rural areas and $3 - 5km$ in urban areas. Their work demonstrates these technologies can be suitable for relatively harsh outdoor environments. Some Wireless WAN communication technologies, including Cellular (3G and 4G), Sigfox, LoRa, NB-IoT and LTE-M, are compared in Table 2. Other WAN technologies include Neul, NWave, PLC, Ethernet, Weightless -N, Weightless -P.

4.4.2. Network Communication Technologies

Once data is transferred from the Thing to the access node, the data is available to the Internet to be transported throughout the top three layers of the network using Internet protocols (IP). HTTP and its secure variant HTTPS are the most well known IP, but due to large control data overheads ensuring data reliability, HTTP and HTTPS may not be the most suitable protocols for constrained IoT systems. So alternative and lighter protocols have been developed that are more suitable for constrained IoT systems. Examples include Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), Message Queue Telemetry Transport (MQTT) and Data Distribution Service (DDS). Some of these protocols offer security feature similar to HTTPS.

Platform	Focus / Tools	Local/ Cloud	Language	Cost ($): Free Vs 10,000 Connected Devices
Ayla Network	E2E. Compatible: AMAP. Tools: embedded agents, Phone-as-a-Gateway, ADP	PaaS	C, Java	Custom pricing
Arm MBED IoT Platform	Compatible: MBED OS. Support: ARM/ARMcommunity. Tools: security E2E, easy integration, open standards	PaaS, local OS	C/C++	Custom pricing
AWS IoT	E2E. Focus: extreme scalability, many partners. Tools: recognition registry for Things, device SDKs, rules engine - message evaluation	IaaS	NET, Java, JVM, Node. js, Python, Ruby, PHP	**Free**: 50 Devices. Daily: 300 msg, 130 registry actions, 150 exceptions **10,000 Devices**: 1 KB msg/min = $560/month [18]
Bosch IoT Suite	E2E. Focus: cost, local&cloud, security. Tools: analytics, open standards	PaaS, local	Unknown	Custom pricing

Table 3: Enterprise IoT Management Platforms (Continued over page)

Platform	Focus / Tools	Local/ Cloud	Language	Cost ($): Free Vs 10,000 Connected Devices
Carriots	Focus: customer access hierachy, easy tool/app integration. Tools: debug/logs, data export, SDKs, API design	PaaS	Groovy	**Free**: 2 Devices, 500 msg/day, 5 KB/msg **10,000 Devices**: $2/Device (up to 1 MB/day) = $20,000/month [28]
Cisco IoT Cloud Connect	Focus: agriculture, customer relations. Tools: Devices connect through cellular (sim) network , voice/data connectivity	PaaS	Unknown	Custom pricing
Datav by Bsquare	Tools: predict/analyse issues, automate maintenance/repairs, max utilisation	PaaS	Unknown	Custom pricing
General Electric's Predix	Compatible: GE apps, products, partners. Focus: healthcare, transport, energy. Tools: asset digital twin modelling	PaaS	Java, Ruby, Node.js, Python	Custom pricing
Google Cloud	E2E. Tools: partnerships with device /app providers, big data analytics, Google's fast fibre network	IaaS	PHP, Java, Node.js, .Net, Ruby, Go, Python	**Free**: 50 Devices, 2800 msg/day (upto 250 MB, then charged minutely) **10,000 Devices**: 1 KB msg/min = $1940/month. [45]
Universal of Things HP	Focus: scalability. Tools: 'market place' for billing, easy app design, analytics	PaaS, local	Unknown	Custom pricing

Table 3: Enterprise IoT Management Platforms (Continued over page)

Platform	Focus / Tools	Local/ Cloud	Language	Cost ($): Free Vs 10,000 Connected Devices
IBM Watson IoT Platform	Compatible: IBM Bluemix. Focus: beginners. Tools: ADP, security, weather data, real-time data, significant storage	PaaS	Java, C, C#, mBed-C++, Python, Node.js/ RED	**Free**: 50 Devices, 1920 msg/day (100 MB/month) **10,000 Devices**: 1 K msg/min = $421.68/month [55]
Kaa IoT Platform	Focus: open source, scalability, industry, low R&D time/cost. Tools: SDKs	PaaS	Java, C, C++ ObjectiveC	Free
LTI's Mosiac	Focus: oil/gas, security/risk compliance, manufacturing. Tools: analytics, insight	PaaS	Unknown	Custom pricing
Microsoft Azure IoT	E2E. Focus: AWS competitor. Tools: rule evaluation engine, device security shadowing, real-time analytics	IaaS	C, Node.js, Java, .NET, Python	**Free**: 50 Devices, 144 msg/day (8 K/day) **10,000 Devices**: (Tier S3) 1 KB msg/min = $3726.55/month [86]
Mocana	Focus: Military level security and tools	PaaS	Unknown	Customised pricing
Oracle Integration Cloud	Focus: manufacturing, logistics, security, scalability. Tools: device virtualisation, big data analytics, fast messaging.	PaaS	Java, Java Script, Node.js	**10,000 Devices**: from $1.6129/hour = $1161.28/month [96]
PTC ThingWorx	Focus: fast develop/deploy. Tools: big data analytics, machine learning, deployable in Device/local/cloud	PaaS, local	C, Java, .NET, iOS, Android	Custom pricing

Table 3: Enterprise IoT Management Platforms (Continued over page)

Platform	Focus / Tools	Local/ Cloud	Language	Cost ($): Free Vs 10,000 Connected Devices
Salesforce IoT Cloud	Focus: capture sales leads, customer relations. Tools: CS management, automate: service request, repair, feedback	PaaS	Rubyon Rails, Java, Node.js, Python,	$4000/month
Samsung Artik	Focus: security, easy to use, optimum system performance	PaaS	PHP, Java, Swift, C++	**Free**: 50 Devices, 72 msg/day (100 K msg/month)
Cloud			Ruby, Java-Android, Python, C	**10,000 Devices**: (Small Business Tier) 1 msg/min = $6480/month [105]
Siemens Mindsphere	Focus: cost-effective, open source based, security. Tools: machine data, confidential storage, embedded agents, libraries	PaaS	Unknown	Custom Pricing comprised of Connectivity, Access and Data

Table 3: Enterprise IoT Management Platforms

4.5. IoT Technologies within the Application Support Layer

Device management, data analysis and processing is handled within the application support layer. For systems with more than a few connected Things, a management platform can handle these tasks. In 2017 more than 450 companies offered IoT Platforms [62]. Platforms can specialise in End-to-End (E2E) solutions, system security, application enablement, device management, analytics, cloud storage and back-end connectivity.

A management platform should enable the following actions or services:

- Synchronise with and monitor connected Things
- Control and retrieve data from Things
- Respond to received data

- Manage system security
- Offer device dashboards to review analytics

Table 3 compares 20 enterprise IoT platforms [111], considering their focus, tools, development languages, and what IoT system can be developed and operated using any free allowance, versus the cost to run a system with 10,000 connected devices. The cost comparison for a 10,000 device system includes each device sending a message once per minute, but excludes data processing, data analysis, device shadowing, rule triggering and other actions which can add additional costs. Developers might need to do further research and testing to determine which platform is best to manage their network.

4.6. IoT Technologies within the Application Presentation Layer

The technology within the Application Presentation Layer includes the Application Development Platform (ADP), which is a tool to enable developers to create and manage end-user software applications. The end-user applications consume the data that was collected by connected sensors and processed in the previous layers, and then present it to the user in a usable format. Some management platforms considered in Section 4.5 include ADPs, for example ThingWorx, Carriots and Kaa. Other management platforms interface with specific ADPs, for example IBM's Watson Management Platform interfaces with IBM's IoT ADP. Additionally, many management platforms also integrate with third party ADPs.

The ADP tools are briefly introduced below. A detailed review is carried out by Ray et al. [101]. Within an ADP, tools can include an Application Programming Interface (API) and Software Development Kits (SDK). In general terms, an API is a block of code acting as an interface between two different objects to enable them to communicate. The API usually comprises of commands, functions and protocols. Within IoT, an API is the code which acts as a logical connector and translator between the connected Thing and an end-user software application enabling easy integration of the Thing into the IoT system and end-user application. Essentially, the API allows the application to access useful processed data. Generally, APIs are created by the manufacture of the IoT Thing.

In some literature, the terms API and SDK are used interchangeably, but they are very different. An SDK is not just code, but instead it is comprised of a whole set of development tools for example libraries, instruction documentation, APIs, samples of code and examples of processes. It may also include ADP guides to help a developer build end-user applications on a specific platform. Additional documentation within the SDK can include industry or user-specific guides. Comparatively, if an API is

thought of as a building block, an SDK can be thought of as a complete workshop full of all of the tools, instructions and building blocks. An API, or multiple APIs can be part of an SDK. Generally, manufacturers create the initial SDK for an IoT device, and developers can contribute to the SDK. Developer contributions are particularly common in an open source environment.

Many ADPs require the developer to be familiar with some programming languages, for example Node.js, Perl, Python, Java or C. Though some platforms have been developed to encourage non-technical developers to create end-user Apps. An example of two such platform include IBM's IoT platform which uses Node-RED visual modelling layout tool employing drag-and-drop methods to connect hardware devices, APIs and on-line services [93]. Secondly, Mendix ADP also uses simple web and desktop based visual modelling tools [84]. Both platforms state that their tools reduce development complexity, time and cost.

4.7. IoT Security Throughout the Architecture Layers

Historically, IoT security has been an after-thought, rather than being considered throughout the design and development of a system. This after-thought approach has led to huge security problems within IoT networks due to no, or low security in IoT endpoints, within network gateways, and throughout the communication layers [103]. These vulnerabilities have led to attacks such as the 2016 Distributed Denial of Service (DDoS) attack against a small jewellery shop, who were under attack from more than 25000 IoT cameras. This attack was found and mitigated by security firm Sucuri [32]. Another very well known example is the Mirai DDoS attack in 2016 [39, 58] which caused Dyn, a large US network provider to temporarily cease providing IT services to its business customers including Amazon, Twitter, PayPal and Netflix, and as a result disabling customer websites. During both the Sucuri and Mirai attacks, hackers used active attack methods [53] to infiltrate a huge number of no-security, or low-security IoT devices and converted them into remotely controlled robots, known as botnets. These botnets were then used to look for other low security IoT devices before all of the botnets were then directed to carry out a DDoS cyber attack on both the Jewellers and Dyn causing the systems to overload with too much traffic. In order to understand the security challenges within IoT systems, this section will consider some common security weaknesses, where the weaknesses sits within the IoT Architecture [127] shown in Figure 2B, the nature of attacks and a range of solutions.

Two important definitions are that of passive and active security attacks. A passive attack can be defined as activity where an unauthorised user, referred to as an attacker, attempts to read data within a network. This action is passive since the

attacker does not attempt to make changes to the data. In comparison, an active attack is when an attacker makes efforts to change data within the network. In both passive and active attacks, the behaviour is unauthorised and for malicious purposes.

4.7.1. Security within Perception Layer & Network Access Layer

The Perception Layer comprises of the sensors and actuators. The Network Access Layer comprises of transmission nodes that allow the access of data into the IoT gateway. Security attacks within these layers are typically the easiest to execute and are generally focused on the acquisition of data. The purpose of attacks in these layers are (1) to snoop on and collect data, (2) to stop sensor from functioning, which can cause a partial denial of service (3) replace sensor data with false data. Sensor snooping is generally a passive attacks, for example employing node capture and eavesdropping techniques [77]. In comparison, active attacks such as hardware jamming can be applied to stop sensors from functioning, or false data injection [53] can be used to replace the sensor data with false data, this in turn may affect the response of the IoT system.

Tools such as Attify can be used to intercept data that is collected by a sensor and transmitted to its node, or from the node to gateway. The attacker may use this data for reconnaissance enabling them to learn about the environment that the sensor is monitoring, or to enable the attacker to perform attacks in other layers of the network.

Another attack method is hardware jamming. Constrained IoT sensors are particularly susceptible to this type of attack which can be achieved in two ways; firstly by remotely injecting the sensor with code or secondly, by physically attaching unauthorised hardware to the sensor to jam it. Hardware jamming is applied for two purposes, to permanently damage the hardware sensor which will reduce or remove its computational power and stop the sensor from collecting data or converting its analogue data into digital data, known as actuating. In this way, hardware jamming can effectively remove sensors from the network, resulting in a sensor DoS. Alternatively, hardware jamming can be used to get vital data such as the cryptographic key or routing table, or to insert false sensor data into the system to affect the behaviour of the IoT system.

A sensor battery-depletion attack is another attack method which is similar to hardware jamming. An attacker can purposely reduce a sensor or actuator's power level, enabling the attacker to reduce its computational power, this can affect the sensor or actuator's ability to function, for example affecting reliable sensing, actuation or communication [108, 109] enabling an attacker to create a sensor or actuator DoS or. Alternatively, if a battery-depletion attack is applied to a sensor, the attacker

can insert false code, which could in turn affect the behaviour of the IoT system.

A relay attack is when an attacker eavesdrops on the communication between the sensor and its node or node and connected gateway. The compromised data is then relayed to another system, a victim system, to make the victim system carry out actions defined by the attacker [99]. Due to the significant growth of constrained IoT devices, this type of attack is increasing in frequency.

Security techniques and strategies to defend against all of these attacks include changing default passwords, device/system authentication, strict firewall rules, static code analysis (SCA) executed within the IoT system or applications and network intrusion detection mechanisms. Authentication of all connected IoT devices is a mitigation method used to reduce the likelihood of malicious devices infiltrating the network. Similarly, safe booting is the technique of checking the integrity of the different operating system (OS) in connected IoT devices, it uses cryptographic hash algorithms. For IoT devices with limited power and computation power, WH and NH cryptographic algorithms are the most appropriate for safe booting [9].

4.7.2. Security within Network Layer

The Network Layer routes data around the IoT network. This layer is embedded deeper than the Perception and Network Access Layer so infiltrating this layer is more difficult [73]. Within this layer, the purpose of attacks is to breach the network to intercept the data within it, this is generally done with active attacks [53] and can include gateway attacks, Man-in-the-Middle, ARP cache poisoning, ICMP attacks, Ping of death, Pong attacks and IP spoofing [57, 52].

A gateway attack is similar to a relay attack applied in the perception layer, it can be used to block the connection between the sensors and the internet infrastructure, thus deleting sensor data or redirecting the sensor data, causing damage to the system and causing a DoS [100]. A Man-in-the-Middle attack is widely used to secretly intercept system data and then alter this data, giving the attacker the ability to capture and manipulate data in real time [34]. A sinkhole attack is related to a Man-in-the-middle attack, the attacker employs a vulnerability within the network layer to cause the dropping of delivery packets, thus preventing the packets from reaching their destination. These dropped packets can then be destroyed or redirected to a different destination which is harmful in an IoT environment resulting in a system wide DoS.

In addition to the interception attacks above, malicious control of this layer can enable sophisticated attacks on services within the next layers the Application Support Layer and the Application Layer, including attacking end-user services or applications.

Security techniques to mitigate these attacks include using firewall rules to instigate device white and black lists, enabling randomized algorithms for TCP sequence numbers, using short time to live (TTL) durations for the DNS cache, blocking applications with weak authentication features or forged packet discovery mechanisms [57]. Secure routing is the technique of routing data via multiple paths securely, this can which reduces the error exposure and acts as a network mitigation technique.

4.7.3. Security within Application Support Layer

The Application Support Layer is the brains of the IoT network because it is responsible for the management of devices and data. Many of the attacks within this layer are as a result of security attacks in the lower layers, also attacks not related to the layers below are sometimes similar in nature to the attacks described in lower layers, but some attacks are also independent of other layers. This layer is vulnerable to a broad range of attacks, including sniffing, malicious code injection [116] and particularly denial of service.

Denial of service is the most common attack here due to the significant number of network resources being used in this layer. This means there are many different types of DoS attacks that can be applied to prevent genuine users from being able to access IoT devices, the complete system or specific applications. DoS attacks typically occur by the attacker flooding a victim device, or multiple victim devices, with redundant requests or null sessions, making it impossible for genuine users to access the victim device, just like the famous Mirai attack [98].

This layer is also known to be vulnerable to malicious insider attacks which are performed by an authorised system user who tries to access information from other users or other devices in the IoT network [106]. Once the insider has access to other user accounts or devices, they can carry out unauthorised actions, for example issue unauthorised commands or access system credentials and vital system information, thus enabling the malicious insider to carry out more higher level attacks.

The Application Support Layer contains many of the shared resources, for example routing tables which can serve as an attack vector for attackers to observe shared resources and get the required information to enable them to carry out attacks on other areas of the IoT system. Similarly, third-party tools such as a Platform as a Service (PaaS) based management platform, or cloud computing data processing tools, they provide a third-party web service component which can be used by attackers to breach the IoT environment remotely.

Malware attacks are executed in this layer. Malware is a security program which is secretly placed inside a network to monitor the traffic without the system administrator being aware of it presence. There are a number of different techniques that

an attacker can use to install malware, including phishing emails, but once malware is in place, the data it collects generally enables further higher level attacks.

Many of these different attacks can be mitigated by enforcing robust security features such as strong authentication, intrusion detection mechanisms, traffic encryption and regularly checking that all of the technologies within the system have up-to-date software, and particularly that patches are applied where required [89]. Data fragmentation is also useful as a mitigation technique in which data within this layer can be split into various fragments and stored on different servers or other system locations, thereby reducing the risk of data theft, or rendering the theft as useless [112]. The hyper-safe lock-down of the write memory files and device boot-up and configuration files mitigates against the unauthorised customisation of the files that control the behavior of the IoT system. This lock-down is achieved by using point indexing which constrains changes in data into the pointer indexes [74]. When all of these measures are implemented and regularly checked, this should act as a good security barrier against external attacks.

4.7.4. Security within Application Layer

The Application Layer manages the user applications and provides services from the rest of the IoT system to the user applications. It is through these applications that an IoT system interacts with its users. These applications include smart home systems, smart healthcare, smart tracking and logistics, and smart city infrastructures and applications, to name a few. All of the services provided by this layer are dependent on the data actuated from sensors, communicated by the Network Layer, and, managed and processed by the Application Support Layer. Lots of data is handled by this layer, so vulnerabilities and threats exist from both within the IoT system and from the applications. Most of these threats are focused on manipulating the IoT application for the attacker‘s purposes. Many of the attacks that can be experienced in the previous layers can occur in this layer, but in addition to the previous attacks, there are also client-side application attacks.

Cross Site Scripting (XSS) is an injection attack during which attackers insert a client-side script such as java script to modify the application‘s web interface, enabling the attacker to trigger unwanted behavior and actions in the application, for example the attacker has the ability to completely change the content and behaviour of the user application [8].

A malicious code attack [53] is another attack vector used by attackers to disrupt the services provided by the application layer. It is sent by an attacker and can sometimes be executed by itself or triggered by the victim through another medium, for example through a phishing emails. The purpose of this attack can be to change

the data within a user application or to gain application credentials or other vital system information.

Intentional data loss is a vulnerability that can affect the application layer. Due to the large amount of data transmitted between the devices, an attacker can orchestrate a disruption in the network which can lead to data loss. In these circumstances, low-cost sensors and actuators are most affected as they generally do not have storage, error checking or redundancy features due to their constrained nature.

Another kind of phishing attack is prevalent in this layer. The attack is distributed through infected user emails with the purpose of tricking a victim into revealing their login credentials, or to tricking the application into accepted spoofed user credentials.

Many of the attacks experienced within the Application Layer occur due to non-standard application code which is written by the application programmer. Generally application programmers are concerned with application functionality rather than security, therefore secure coding techniques may not be employed. This non-standard code increases application vulnerabilities allowing malicious attackers to take advantage and cause damage to the IoT system.

The majority of these attacks can be mitigated with 'user validation' using integrity and encryption mechanisms to authenticate user interactions. The use of system anti-virus, firewalls and anti-malware programs are crucial. Finally, incoming and outgoing network traffic can be monitored, also, for a large scale IoT system, all of the sensor and actuator connections within the system can be monitored. All of these interactions can be monitored using systems such as a Network Intrusion Detection (NID) system. For most networks and IoT systems there are 'normal traffic' patterns, and the NID system can be trained to recognise normal traffic and detect outliers or anomalies.

5. Future Developments

As discussed throughout this paper, IoT can be used to target challenges and improve quality of life. In the opinion of the authors, one of the largest international challenges that we face today is this that of reducing energy consumption. Energy has become a very important human commodity. Yet, it is widely recognised that our main energy resources, that of coal, gas and oil are limited. So, there is the need to find alternative sustainable energy resources and to reduce energy consumption. Instead though, Worldwide, energy consumption is currently increasing, particularly in the world's emerging markets. Since the 1970s Asia and Africa's energy demands have increased approximately 7 fold [61]. In addition to these factors, at present,

"most people spend 90% of their daily lives indoors relying on mechanical heating and air conditioning, thus leading to buildings becoming the largest energy consumers worldwide" [27]. Within the US and the EU, buildings account for a staggering 40% of all of the energy that is consumed this those regions.

Existing Building Energy Management Systems (BEMS) generally measure and monitor energy usage. Some systems also offer automated control of the Heating, Ventilation and Air Conditioning (HVAC) Systems. These BEMS have been demonstrated to reduce energy consumption by up to 30%. An area of further future development of IoT technology is within advanced BEMS using the concepts of Next Generation Internet, to achieve further energy reductions of $30-40\%$ [19]. Such systems could include additional control, for example to automate opening or closing of windows, doors and other building assets, control of appliances or machinery, for example, turning off domestic appliances when energy consumption passes a usage threshold, or turning industrial machinery from 'stand-by' to 'off' outside working hours. Developments could also include data fusion techniques [3] to combine different IoT data sets, including weather data, zoned heating linked to room occupancy [38, 71], or lighting systems which respond to external daylight conditions [27]. Such system could manage windows and blinds causing windows to tilt slightly to reflect away sunlight during warm conditions, or blinds to open fully to make optimal use of external light conditions. Also, the consideration of the people using these buildings; their comfort and their building interaction expectations [4] AI, machine learning and gamification techniques could be employed to make these systems more intelligent, human-centric and energy conscience, allowing us to reduce energy consumption further. AI and machine learning are methods of increasing system intelligence, including human ethics and improving user experience. Gamification is the mechanics of gaming, applied in a real-life context to improve a user's experience of a system and increase their engagement with it.

Many different and often unrelated IoT BEMS are currently being developed, but future developments that focus on user engagement by including system resilience, delivering sustainability and combining more of these different techniques are most likely to result in consumer and industrial uptake, enabling ae significant reduction in energy consumption within buildings, which will in turn result in a significant reduction in worldwide energy consumption.

6. Conclusion

This paper seeks to be an introduction, overview, and reference guide for IoT systems, particularly considering security issues. Within this paper the authors

demonstrate that IoT is the culmination of advances within computing, communication technologies and the Internet, all combined with the human drive to improve our quality of life. Next, IoT architectures and technologies are introduced including a number of quick reference technology comparison tables. Following this, the significant IoT security vulnerabilities, which have appeared as a result of the rapid development of IoT are described and some mitigation techniques are discussed. Finally, a future area of development is introduced.

[1] Thomas Aasebo. 2017. Wireless Technology Bluetooth, Zigbee and Ant. (2017). http://its-wiki.no/wiki/

[2] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani. 2016. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications* 23, 5 (October 2016), 10–16. https://doi.org/10.1109/MWC.2016.7721736

[3] Kemal Akkaya, Ismail Guvenc, Ramazan Aygun, Nezih Pala, and Abdullah Kadri. 2015. IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In *Wireless Communications and Networking Conference Workshops (WCNCW), 2015 IEEE*. IEEE, 58–63.

[4] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri. 2015. IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In *2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. 58–63. https://doi.org/10.1109/WCNCW.2015.7122529

[5] A Al-Fuqaha, M Guizani, M Mohammadi, M Aledhari, and M Ayyash. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials* 17, 4 (Fourthquarter 2015), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[6] S Al-Qaseemi, H Almulhim, H Almulhim, and S Chaudhry. 2016. IoT architecture challenges and issues: Lack of standardization. In *2016 Future Technologies Conference (FTC)*. 731–738. https://doi.org/10.1109/FTC.2016.7821686

[7] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. Internet of Things security: A survey. *Journal of Network and Computer Applications* 88 (2017), 10–28.

[8] Bako Ali and Ali Awad. 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* 18, 3 (2018), 817.

[9] MOJTABA Alizadeh, Mazleena Salleh, Mazdak Zamani, Jafar Shayan, and Sasan Karamizadeh. 2012. Security and performance evaluation of lightweight cryptographic algorithms in RFID. *Communications and Computing* (2012), 45–50.

[10] Leonardo Albernaz Amaral, Everton de Matos, Ramão Tiago Tiburski, Fabiano Hessel, Willian Tessaro Lunardi, and Sabrina Marczak. 2016. Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G. In *Internet of Things (IoT) in 5G Mobile Technologies*. Springer, 333–367.

[11] Michael Andersen. 2015. Trends in Internet of Things platforms. *XRDS: Crossroads, The ACM Magazine for Students* 22, 2 (2015), 40–43.

[12] Kevin Ashton. 2009. That 'Internet of Things' Thing. *RFiD Journal* 22, 7 (2009), 97–114.

[13] IEEE Standards Association et al. [n. d.]. P2413.1 - Standard for a Reference Architecture for Smart City (RASC). ([n. d.]). https://standards.ieee.org/project/2413$_1$.*html*

[14] IEEE Standards Association et al. 2016. P2413-Standard for an Architectural Framework for the Internet of Things (IoT). *Institute of Electrical and Electronics Engineers, New York* (2016).

[15] AT&T. 2013. Comparing LTE and 3G Energy Consumption. (2013). https://developer.att.com/application-resource-optimizer/docs/best-practices/comparing-lte-and-3g-energy-consumption

[16] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A Survey. *Computer Networks* 54, 15 (2010), 2787–2805.

[17] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2017. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks* 56 (2017), 122–140.

[18] AWS. 2017. AWS IoT Core Pricing. (2017). https://aws.amazon.com/IoT-core/pricing/

[19] Bharathan Balaji, Jian Xu, Anthony Nwokafor, Rajesh Gupta, and Yuvraj Agarwal. 2013. Sentinel: occupancy based HVAC actuation using existing WiFi infrastructure within commercial buildings. In *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*. ACM, 17.

[20] John Barber. 2017. Getting Answers to Your IoT Questions. (2017). http:www.gartner.com/podcasts/getting-answers-to-your-IoT-questions/

[21] Peter Barker and Mohammad Hammoudeh. 2017. A Survey on Low Power Network Protocols for the Internet of Things and Wireless Sensor Networks. In *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 33.

[22] Simon Elias Bibri and John Krogstie. 2017. Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustainable Cities and Society* 31 (2017), 183–212.

[23] JM Blythe and SD Johnson. 2018. The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. (2018).

[24] Tuhin Borgohain, Uday Kumar, and Sugata Sanyal. 2015. Survey of Operating Systems for the IoT Environment. *CoRR* abs/1504.02517 (2015).

[25] M Botterman. 2009. For the European Commission Information Society and Media Directorate General. In *Networked Enterprise & RFID Unit–D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic*.

[26] Armir Bujari, Marco Furini, Federica Mandreoli, Riccardo Martoglia, Manuela Montangero, and Daniele Ronzani. 2018. Standards, Security and Business Models: Key Challenges for the IoT Scenario. *Mobile Networks and Applications* 23, 1 (01 Feb 2018), 147–154. https://doi.org/10.1007/s11036-017-0835-8

[27] Xiaodong Cao, Xilei Dai, and Junjie Liu. 2016. Building energy-consumption status worldwide and the state-of-the-art technologies for zero-energy buildings during the past decade. *Energy and buildings* 128 (2016), 198–213.

[28] Carriots. 2017. Carriots Pricing. (2017). https://www.carriots.com/pricing

[29] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2016. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* 23, 5 (2016), 60–67.

[30] Tej Bahadur Chandra, Pushpak Verma, and A. K. Dwivedi. 2016. Operating Systems for Internet of Things: A Comparative Study. In *Proceedings of the*

Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). ACM, New York, NY, USA, Article 47, 6 pages. https://doi.org/10.1145/2905055.2905105

[31] Khyati Chourasia, Anubhuti Khare, Manish Saxena, and Roshan Singh Thakur. 2012. Conserving Energy in 3G and Study of 4G Cellular Networks. (2012).

[32] Daniel Cid. [n. d.]. Large CCTV Botnet Leveraged in DDoS Attacks. ([n. d.]). https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

[33] Cisco. 2015. Internet of Things Will Deliver $1.9 Trillion Boost To Supply Chain And Logistics Operations. (2015). https://newsroom.cisco.com/press-release-content?articleId=1621819

[34] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. 2016. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 2027–2051.

[35] British Government: DDCMS. [n. d.]. Government response to the Secure by Design informal consultation. ([n. d.]). https://www.gov.uk/government/publications/secure-by-design/government-response-to-the-secure-by-design-informal-consultation

[36] British Government: DDCMS. 2018. *Code of Practice for Consumer IoT Security*. British Government.

[37] British Government: DDCMS. 2019. Open consultation: Consultation on regulatory proposals on consumer IoT security. (2019). https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

[38] S. Dharur, C. Hota, and K. Swaminathan. 2017. Energy efficient IoT framework for Smart Buildings. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. 793–800. https://doi.org/10.1109/I-SMAC.2017.8058288

[39] Dyn. 2016. Dyn Analysis Summary Of Friday October 21 Attack. (2016). https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[40] Ericsson. 2016. Ericsson Mobility Report 2016. *Ericsson, Stockholm, Sweden, Tech. Rep. EAB-16* (2016).

[41] Internationale Fernmeldeunion. 2012. ITU-T Y. 4000/Y. 2060 (06/2012). *Overview of the Internet of things* (06 2012).

[42] Gartner. 2018. Internet of Things Definition. (2018). www.gartner.com/it-glossary/Internet-of-things/

[43] Neil Gershenfeld and JP Vasseur. 2014. As objects go online; the promise (and pitfalls) of the Internet of Things. *Foreign Aff.* 93 (2014), 60.

[44] Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, and Thar Baker. 2018. Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing* (2018), 1–17.

[45] Google. 2017. Google Cloud Internet of Things Core Pricing. (2017). https://cloud.google.com/iot/pricing

[46] Google. 2017. Overview of Internet of Things. (2017). https://cloud.google.com/solutions/iot-overview

[47] J. Granjal, E. Monteiro, and J. S Silva. 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys Tutorials* 17, 3 (thirdquarter 2015), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

[48] GS1. 2017. GS1 And The Internet of Things. (2017). https://www.gs1.org/sites/default/files/images/standards/internet-of-things/gs1-and-the-internet-of-things-iot.pdf

[49] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems* 29, 7 (2013), 1645–1660.

[50] Brij Gupta, Dharma P Agrawal, and Shingo Yamaguchi. 2016. *Handbook of research on modern cryptographic solutions for computer and cyber security.* IGI global.

[51] Brij B Gupta. 2018. *Computer and cyber security: principles, algorithm, applications, and perspectives.* CRC Press.

[52] Asif Habib. 2008. Sensor network security issues at network layer. In *Advances in Space Technologies, 2008. ICAST 2008. 2nd International Conference on*. IEEE, 58–63.

[53] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu. 2018. Privacy in the Internet of Things for Smart Healthcare. *IEEE Communications Magazine* 56, 4 (APRIL 2018), 38–44. https://doi.org/10.1109/MCOM.2018.1700809

[54] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel. 2018. Survey of platforms for massive IoT. In *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*. 1–8. https://doi.org/10.1109/FIoT.2018.8325598

[55] IBM. 2017. IoT Cost Calculator. (2017). https://console.bluemix.net/pricing/platform/internet$_of_things$

[56] IEEE. 2014. Special Report: The Internet of Things. *IEEE The Institute* March (2014). http://theinstitute.ieee.org/static/special-report-the-internet-of-things

[57] M Imani, M Taheri, ME Rajabi, and M Naderi. 2010. Vulnerabilities in network layer at wireless mesh networks (WMNs). In *Educational and Network Technology (ICENT), 2010 International Conference on*. IEEE, 487–492.

[58] Incapsula. 2016. Breaking Down Mirai: An IoT DDoS Botnet Analysis. (2016). https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[59] INFSO Networked Enterprise & RFID INFSO. 2008. Internet of Things in 2020, Roadmap for the Future, Version 1.1, Authors: INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems in co-operation with the RFID Working Group Of EPOSS. (2008).

[60] Next Generation Internet Initiative. [n. d.]. Next Generation Internet - Vision. ([n. d.]). https://www.ngi.eu/vision/

[61] International Energy Agency. 2016. *World Energy Balances 2016*. OECD.

[62] IoT Analytics. 2017. List Of 450 IoT Platform Companies. (2017). https://IoT-analytics.com/product/list-of-450-IoT-platform-companies/

[63] ISO/IEC/IEEE. 2011. ISO/IEC/IEEE Systems and software engineering – Architecture description. *ISO/IEC/IEEE 42010:2011(E) (Revision of ISO/IEC 42010:2007 and IEEE Std 1471-2000)* (Dec 2011), 1–46. https://doi.org/10.1109/IEEESTD.2011.6129467

[64] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q1/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=13670

[65] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q3/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=14126

[66] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q3/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=14650

[67] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q6/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=14656

[68] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q6/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=14318

[69] ITU. 2018. ITU Work Program [2017-2020]:[SG20]:[Q7/20]. (2018). https://www.itu.int/ITU-T/workprog/wp_item.aspxisn=14949

[70] Mike Jenks, Elizabeth Burton, and Katie Williams. 1996. A sustainable future through the compact city? Urban intensification in the United Kingdom. *Environment by Design* 1, 1 (1996), 5–20.

[71] Ming Jin, Nikolaos Bekiaris-Liberis, Kevin Weekly, Costas Spanos, and Alexandre Bayen. 2015. Sensing by proxy: Occupancy detection based on indoor CO2 concentration. *UBICOMM 2015* 14 (2015).

[72] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, and Jesus Alonso-Zarate. 2015. A survey on application layer protocols for the Internet of Things. *Transaction on IoT and Cloud Computing* 3, 1 (2015), 11–17.

[73] Chris Karlof and David Wagner. 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks* 1, 2-3 (2003), 293–315.

[74] Sarvesh Kumar, Suraj Pal Singh, A Kumar Singh, and Jahangir Ali. 2013. Virtualization, the great thing and issues in cloud computing. *International Journal of Current Engineering and Technology* 3 (2013).

[75] LB Landauer. 2001. The History, Development, and Importance of Personal Computers. *Science and Its Times: Understanding the Social Significance of Scientific Discovery* 7 (2001), 536–540.

[76] Christian Ostergaard Laursen. 2017. Internet of Things: A Comparison of Communication Technologies. (2017). https://blog.montem.io/2017/03/10/Internet-of-things-a-comparison-of-communication-technologies/

[77] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal* 4, 5 (Oct 2017), 1125–1142. https://doi.org/10.1109/JIoT.2017.2683200

[78] SW Lin, B Miller, J Durand, G Bleakley, A Chigani, R Martin, B Murphy, and M Crawford. 2017. IIC: The industrial internet of things volume G1: reference architecture. *Industrial Internet Consortium* (2017), 10–46.

[79] James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. 2015. Unlocking the Potential of the Internet of Things. *McKinsey Global Institute* (2015).

[80] Johan Marconot, Florian Pebay-Peyroula, and David Hély. 2017. IoT Components LifeCycle Based Security Analysis. In *2017 Euromicro Conference on Digital System Design (DSD)*. IEEE, 295–298.

[81] IHS Markit and Sam Lucero. 2016. IoT platforms: Enabling the Internet of Things. *HIS Technology* March (2016).

[82] Maria-Lluïsa Marsal-Llacuna, Joan Colomer-Llinàs, and Joaquim Meléndez-Frigola. 2015. Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative. *Technological Forecasting and Social Change* 90 (2015), 611–622.

[83] C. A. Medina, M. R. Prez, and L. C. Trujillo. 2017. IoT Paradigm into the Smart City Vision: A Survey. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 695–704. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.109

[84] Mendix. 2017. Collaborative Visual Development. (2017). https://www.mendix.com/collaborative-visual-development/

[85] Wu Miao, Lu Ting-Jie, Ling Fei-Yang, Sun Jing, and Du Hui-Ying. 2010. Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, Vol. 5. V5–484–V5–487. https://doi.org/10.1109/ICACTE.2010.5579493

[86] Microsoft Azure. 2017. Pricing Calculator. (2017). https://azure.microsoft.com/en-gb/pricing

[87] Roberto Minerva, Abyi Biru, and Domenico Rotondi. 2015. Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative* 1 (2015).

[88] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497 – 1516. http://www.sciencedirect.com/science/article/pii/S1570870512000674

[89] Alhasan A. Alharbi Mohammed Tawfik, Ali M. Almadni. 2017. A Review: the Risks And weakness Security on the IoT. *IOSR Journal of Computer Engineering* 1 (2017), 12–17.

[90] Manuela Montangero. 2017. IoT: Science Fiction or Real Revolution?. In *Smart Objects and Technologies for Social Good: Second International Conference, GOODTECHS 2016, Venice, Italy, November 30–December 1, 2016, Proceedings*, Vol. 195. Springer, 96.

[91] Bill Morelli. 2013. Internet Connected Devices: Evolving from the "Internet of Things to the "Internet of Everything. *IHS Website* (2013). https://www.ihs.com/pdf/IHS-IoT-Evolution_161384110915583632.pdf

[92] Max HA Newman. 1955. Alan Mathison Turing. 1912-1954. *Biographical memoirs of Fellows of the Royal Society* 1 (1955), 253–263.

[93] NodeRED. 2017. NodeRED. (2017). https://nodered.org/

[94] K. E. Nolan, Y. Guibene, and M. Y. Kelly. 2016. An evaluation of low power wide area network technologies for the Internet of Things. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. 439–444. https://doi.org/10.1109/IWCMC.2016.7577098

[95] Adegboyega Ojo, Edward Curry, Tomasz Janowski, and Zamira Dzhusupova. 2015. *Designing Next Generation Smart City Initiatives - The SCID Framework*. https://doi.org/10.1007/978-3-319-03167-5_4

[96] Oracle. 2017. Oracle Integration Cloud Pricing. (2017). https://oracle.com/

[97] N Oyj. 2016. LTE evolution for IoT connectivity. *Nokia Corporation White Paper* (2016).

[98] S Prabhakar. 2017. Network Security in Digitalization: Attacks and Defence. *Int. J. Res. Comput. Appl. Robot* 5, 5 (2017), 46–52.

[99] Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen. 2016. Threats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Computing* 3, 3 (2016), 64–71.

[100] Tariq Aziz Rao. 2018. Security Challenges Facing IoT Layers and its Protective Measures. *International Journal of Computer Applications* 179 (2018), 8887–8921.

[101] Partha Pratim Ray. 2016. A survey of IoT cloud platforms. *Future Computing and Informatics Journal* 1, 1 (2016), 35 – 46. http://www.sciencedirect.com/science/article/pii/S2314728816300149

[102] C. Sabri, L. Kriaa, and S. L. Azzouz. 2017. Comparison of IoT Constrained Devices Operating Systems: A Survey. In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*. 369–375. https://doi.org/10.1109/AICCSA.2017.187

[103] Jibran Saleem, Bamidele Adebisi, Ruth Ande, and Mohammad Hammoudeh. 2017. A state of the art survey-Impact of cyber attacks on SME's. In *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 52.

[104] Mattia Salnitri, Mahdi Alizadeh, Daniele Giovanella, Nicola Zannone, and Paolo Giorgini. 2018. From Security-by-Design to the Identification of Security-Critical Deviations in Process Executions. In *International Conference on Advanced Information Systems Engineering*. Springer, 218–234.

[105] Samsung. 2017. Pricing Plans. (2017). https://artik.cloud/pricing/

[106] Ameya Sanzgiri and Dipankar Dasgupta. 2016. Classification of insider threat detection techniques. In *Proceedings of the 11th annual cyber and information security research conference*. ACM, 25.

[107] Pallavi Sethi and Smruti R Sarangi. 2017. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering* 2017 (2017).

[108] Vladimir Shakhov and Insoo Koo. 2018. Depletion-of-Battery Attack: Specificity, Modelling and Analysis. *Sensors* 18, 6 (2018), 1849.

[109] Vladimir V Shakhov. 2013. Protecting wireless sensor networks from energy exhausting attacks. In *International Conference on Computational Science and Its Applications*. Springer, 184–193.

[110] Zhengguo Sheng, Shusen Yang, Yifan Yu, Athanasios Vasilakos, Julie Mccann, and Kin Leung. 2013. A survey on the ietf protocol suite for the Internet of Things: Standards, challenges, and opportunities. *IEEE Wireless Communications* 20, 6 (2013), 91–98.

[111] Santosh Singh. 2018. Top 20 IoT Platforms in 2018. (2018). https://Internetofthingswiki.com/top-20-IoT-platforms/

[112] Yashaswi Singh, Farah Kandah, and Weiyi Zhang. 2011. A secured cost-effective multi-cloud storage in cloud computing. In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 619–624.

[113] Ian Skerrett. 2016. Three Software Stacks Required for the Internet of Things (IoT). (2016). https://www.linkedin.com/pulse/three-software-stacks-required-internet-things-iot-eclipse-das

[114] Phil Smith. 2017. Comparing Low-Power Wireless Technologies. (2017). https://www.digikey.co.uk/en/articles/techzone/2017/oct/comparing-low-power-wireless-technologies

[115] Christos Stergiou, Kostas E Psannis, Byung-Gyu Kim, and Brij Gupta. 2018. Secure integration of IoT and cloud computing. *Future Generation Computer Systems* 78 (2018), 964–975.

[116] Sowmya Nagasimha Swamy, Dipti Jadhav, and Nikita Kulkarni. 2017. Security threats in the application layer in IoT applications. In *I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on*. IEEE, 477–480.

[117] Jorg Swetina, Guang Lu, Philip Jacobs, Francois Ennesser, and JaeSeung Song. 2014. Toward a standardized common M2M service layer platform: Introduction to oneM2M. *IEEE Wireless Communications* 21, 3 (2014), 20–26.

[118] Techtarget. 2016. The essential guide to supply chain management best practices. (2016). http://Internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[119] Nadeem Unuth. 2017. What Is the Definition of 3G Wireless Technology? Technical Specifications of 3G. (2017). https://www.lifewire.com/what-is-3g-3426465

[120] Jeffrey Voas. 2016. Networks of things. *NIST Special Publication* 800, 183 (2016), 800–183.

[121] J Voas. 2018. NIST: Internet of Things (IoT) Trust Concerns. (2018).

[122] H Wang and A O Fapojuwo. 2017. A Survey of Enabling Technologies of Low Power and Long Range Machine-to-Machine Communications. *IEEE Communications Surveys Tutorials* 19, 4 (Fourthquarter 2017), 2621–2639. https://doi.org/10.1109/COMST.2017.2721379

[123] Wikipedia. 2017. ANT (network). (2017). https://en.wikipedia.org/wiki/ANT_(*network*)

[124] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. 2017. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal* 4, 5 (Oct 2017), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

[125] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani. 2017. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications* 24, 3 (June 2017), 10–16. https://doi.org/10.1109/MWC.2017.1600421

[126] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. 2014. Internet of Things for Smart Cities. *IEEE Internet of Things Journal* 1, 1 (Feb 2014), 22–32. https://doi.org/10.1109/JIoT.2014.2306328

[127] C. L. Zhong, Z. Zhu, and R. G. Huang. 2015. Study on the IoT Architecture and Gateway Technology. In *2015 14th International Symposium on Distributed*

Computing and Applications for Business Engineering and Science (DCABES). 196–199. https://doi.org/10.1109/DCABES.2015.56